PROXIMA

MCC Workshop

Francisco J. Cazorla

PROXIMA Coordinator(BSC)
Director of the Computer Architecture/Operating System group @ BSC

BSC-UPC, Nov 22nd, 2016

This project and the research leading to these results has received funding from the European Community's Seventh Framework Programme [FP7 / 2007-2013] under grant agreement 611085

www.proxima-project.eu

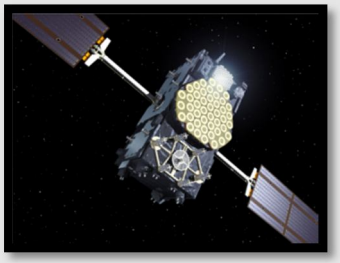
Critical Real Time Embedded Systems (CRTES)

Does the Software work?

Functional correctness	Timing correctness
Software performs its task	Software fits its assigned time budget

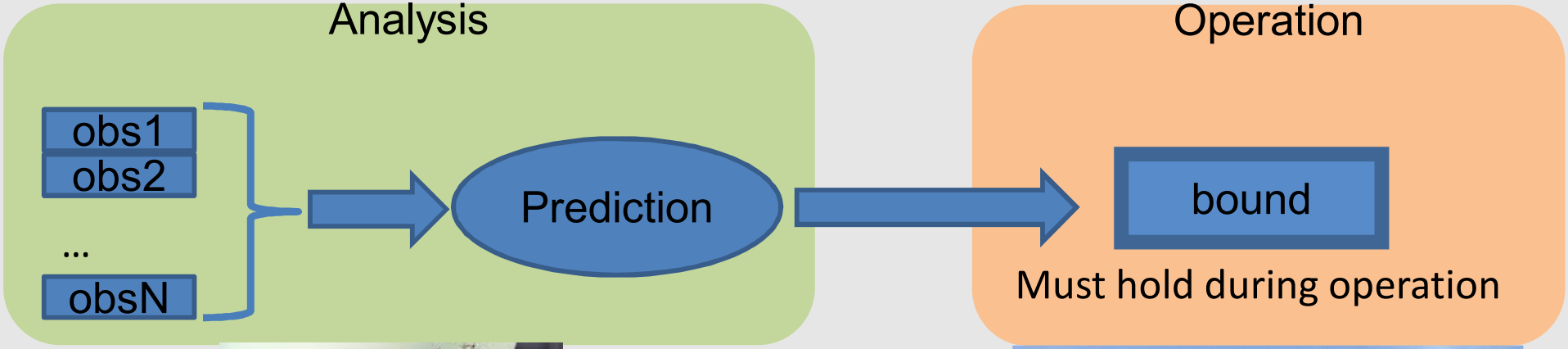
Provide evidence about the functional and timing correctnes of the system (against safety standards)





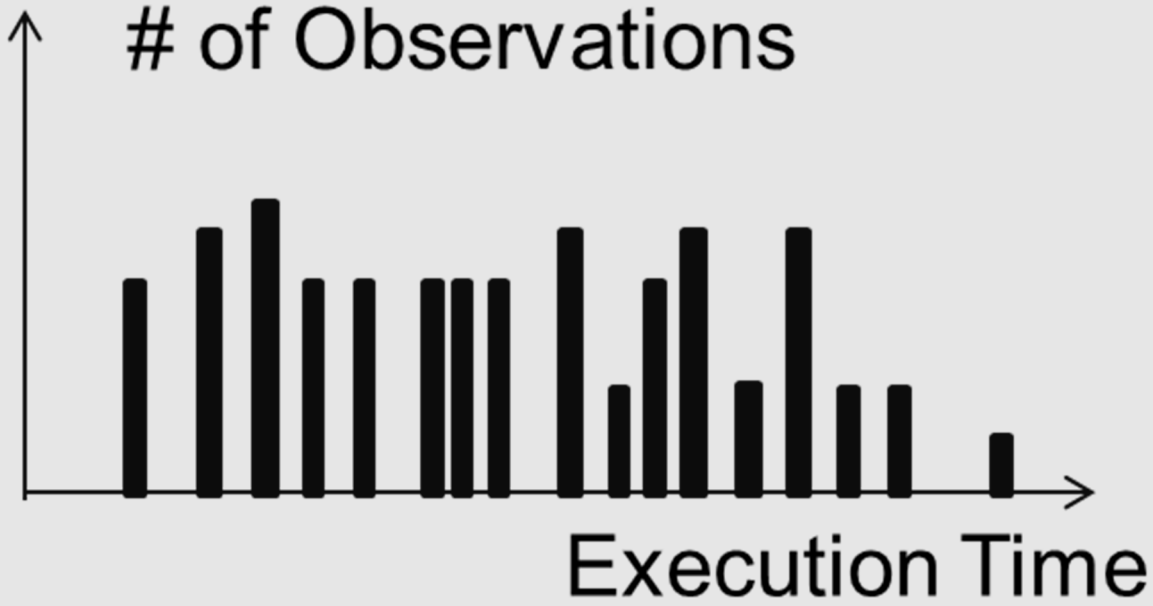

Measurement-Based Timing Analysis

- Dominant timing analysis approach in different segments
- Analysis phase
  - Collect measurements to derive a WCET estimate that holds valid during system operation
- Operation phase
  - Actual use of the system (under assumption is stays within its performance profile)



Sources of Jitter (SoJ)

- Any platform element in the platform that cause execution time of a program to vary
  - SoJ determine the **execution conditions** for each program run
- Systems are complex
  - Users only follow what happens at a high level



Goals

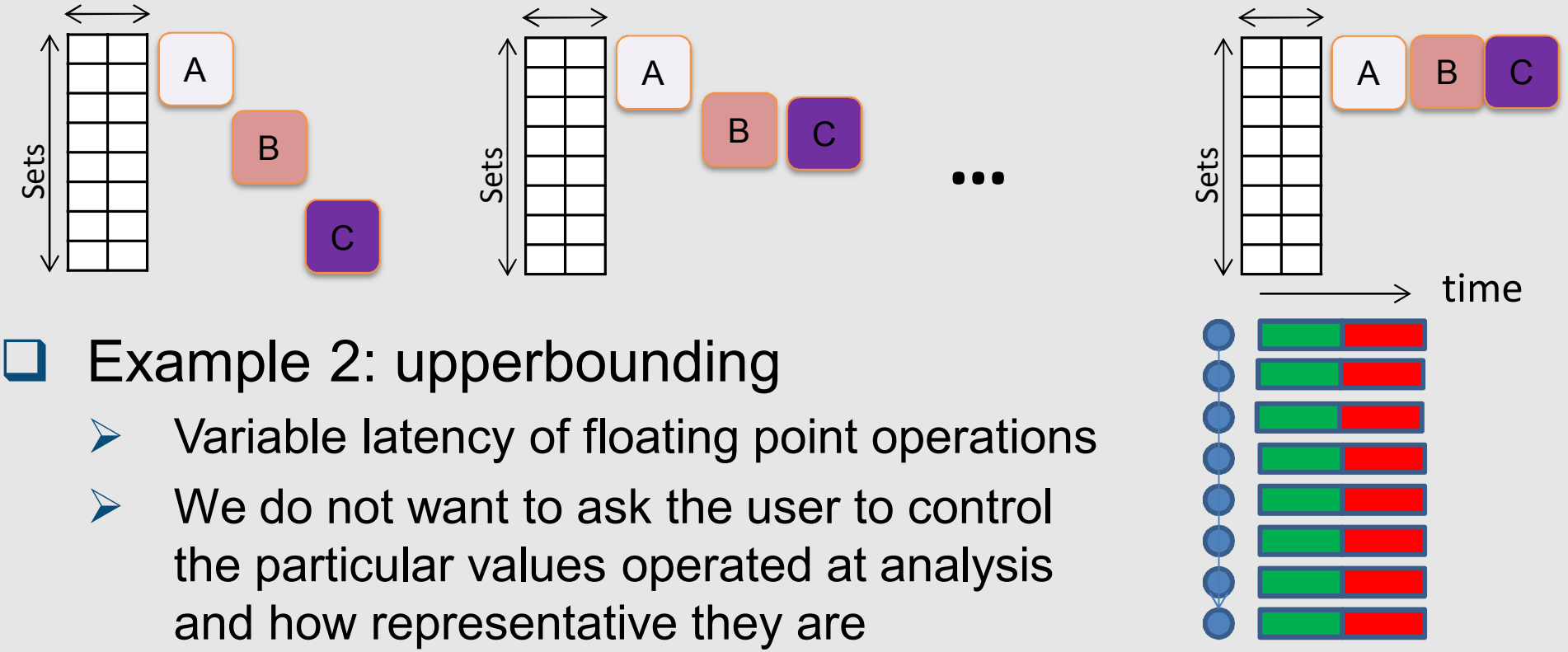
- Accurate and cost-effective timing analysis
- Representative testing
  - Ensure that the worst-case conditions have been exercised or closely approximated
    - Reduce the effort/cost involved
    - Do not require the end user to deal with low-level hardware details
- Get estimates as early as possible during system design
  - Achieve ‘resilient’ (time composability) WCET estimates
    - across incremental integrations
    - at the multicore level

High-level and Low-level SoJ

- **High-level SoJ**: the user has some control on them
  - Input vectors impact on execution paths
    - Metrics to measure coverage (SC, DC, MCDC)
    - Tools to determine coverage
    - Which path was traversed, to make claims on path coverage
- The use of complex high-performance hardware creates other **low-level SoJ**
  - The user lacks means to measure the coverage of low-level SoJ
    - Often insufficient support from the HW

Examples of Low-level SoJ

- Example 1: randomization SW or HW
  - The mapping program objects (functions) →
    - How software objects are assigned to memory →
    - How they are placed in cache → conflicts suffered →
    - Execution-time effects



- Example 2: upperbounding
  - Variable latency of floating point operations
  - We do not want to ask the user to control the particular values operated at analysis and how representative they are

How to handle low-level SoJ

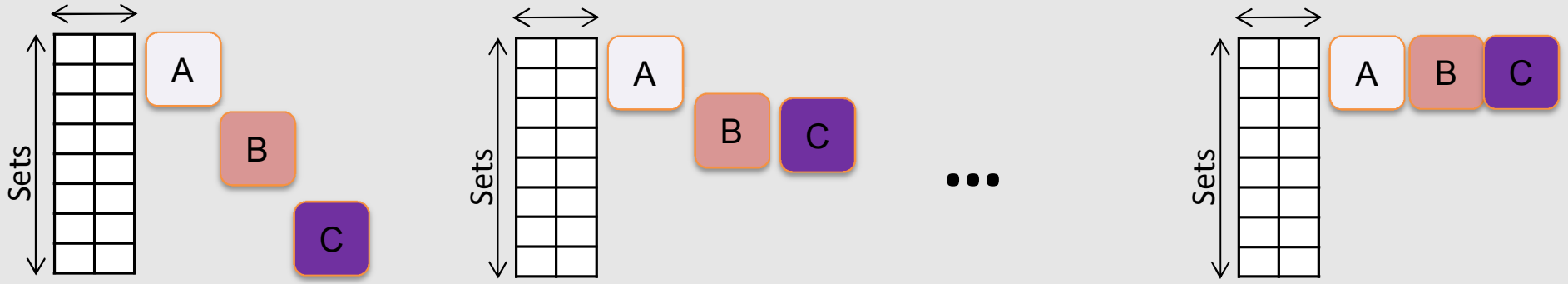
Measurement Based
Probabilistic Timing Analysis

Probabilistic Analysis

Representativeness
- Randomization
- upperobunding

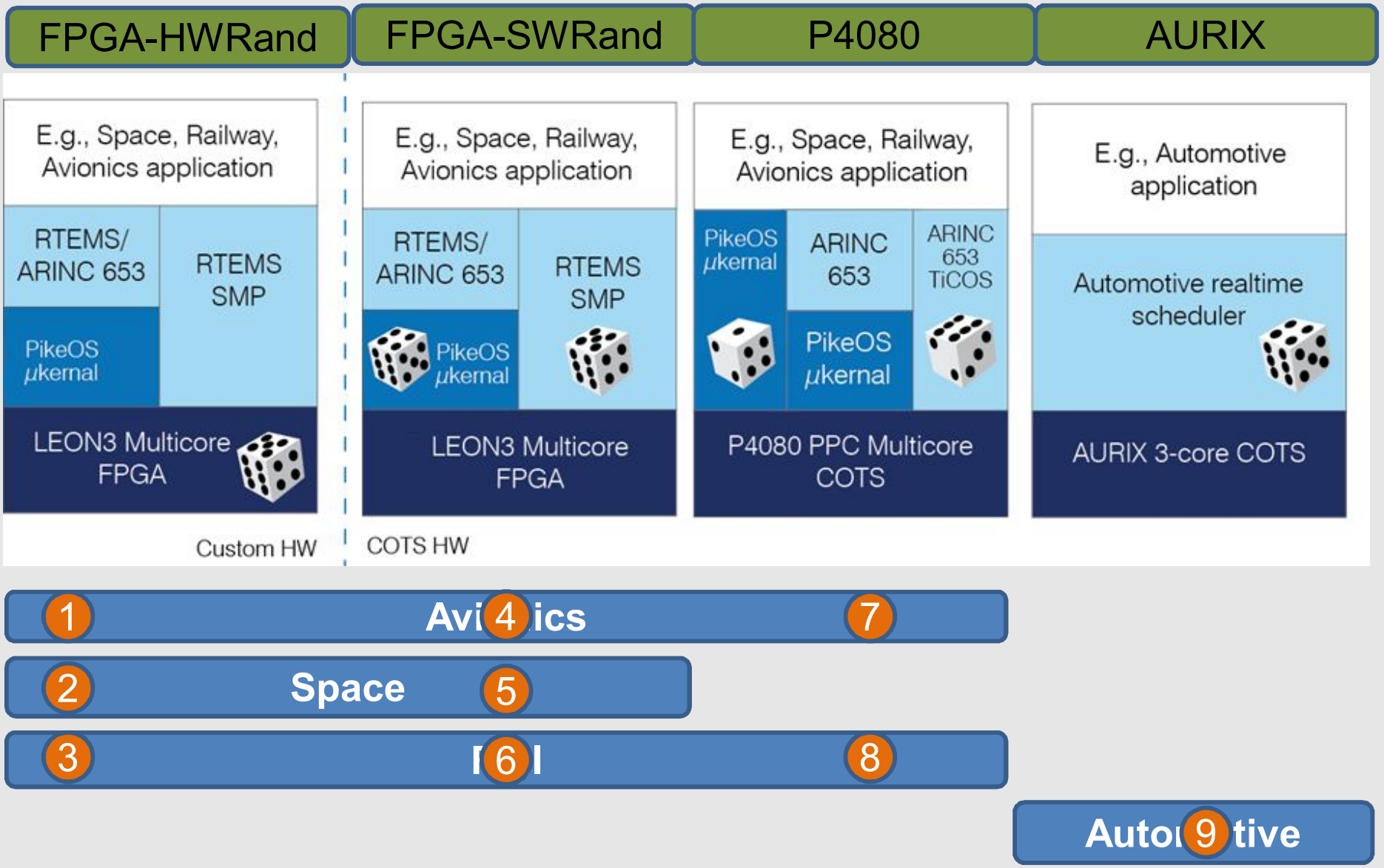
Example: the Cache

- Memory mapping → cache layouts → execution time



- Deterministic system
  - How does the user get confident that experiments capture bad (worst) mappings?
  - Memory mapping varies across runs, but not in a random manner
- Randomized systems
  - Make N runs
  - We can derive
    - the probability of the observed mappings @ operation
    - the probability of unobserved mappings

PROXIMA Platforms and Toolchains



PROXIMA

MCC Workshop

Francisco J. Cazorla

PROXIMA Coordinator(BSC)
Director of the Computer Architecture/Operating System group @ BSC

BSC-UPC, Nov 22nd, 2016

This project and the research leading to these results has received funding from the European Community's Seventh Framework Programme [FP7 / 2007-2013] under grant agreement 611085

www.proxima-project.eu

PROXIMA

Technology Exploitation and Success Stories

Ian Broster

Rapita Systems Ltd

Nov 22nd, 2016

This project and the research leading to these results has received funding from the European Community's Seventh Framework Programme [FP7 / 2007-2013] under grant agreement 611085

www.proxima-project.eu

The PROXIMA Story

Idea

PROARTIS

MBPTA

Technology

PROXIMA

Aerospace

Automotive

Space

Rail

Strategy:

- Build toolchain of technologies
- Apply to COTS/industrial targets using case studies
- Industrial involvement: references and early adopters

What does PROXIMA give me?

- Software timing analysis
  - WCET, low overhead measurement technique
    - Cost effective embedded platforms
- Testing technique for software performance
  - Like sensitivity analysis/mutation testing for timing
    - Reduces risk of timing faults being missed
- Time-composablility
  - Robustness
    - Reduce risk of timing faults nearer integration time

PROXIMA Consortium

Research Partners	Technology Providers	End Users
Barcelona Supercomputing Center Universita Degli Studi Di Padova University of York INRIA	Aeroflex Gaisler Ab Rapita Systems Limited Sysgo S.A.S IKERLAN S.COOP	Airbus Defence and Space Infineon Technologies UK Ltd Airbus Operations SAS

Industrial Advisory Board

Automotive

Rail

Space

PROXIMA

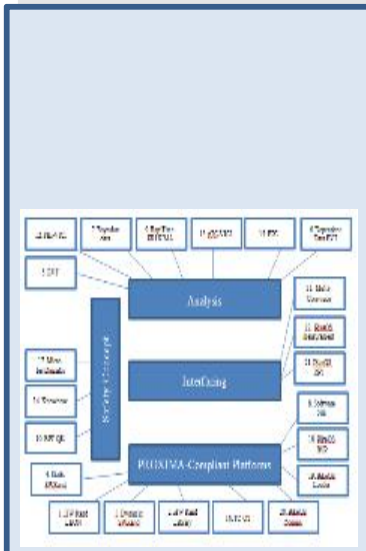
Exploitation Route

PROXIMA Toolchain

Exploitable Technologies

Success Stories

Ecosystem



22

14

many

Research

Early adopters

5

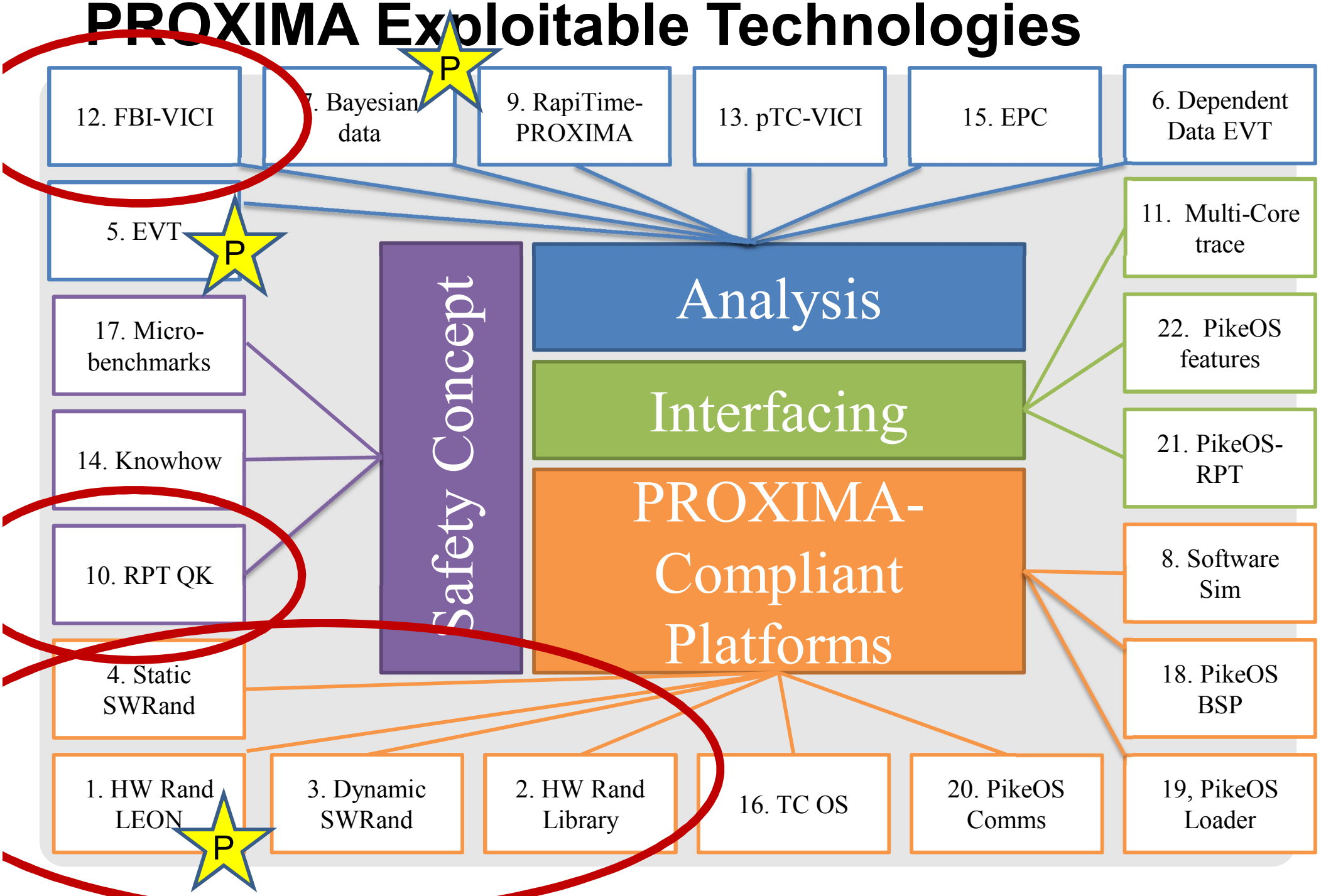
PROXIMA

Exploitable Technologies

This project and the research leading to these results has received funding from the European Community's Seventh Framework Programme [FP7 / 2007-2013] under grant agreement 611085

www.proxima-project.eu

PROXIMA Exploitable Technologies

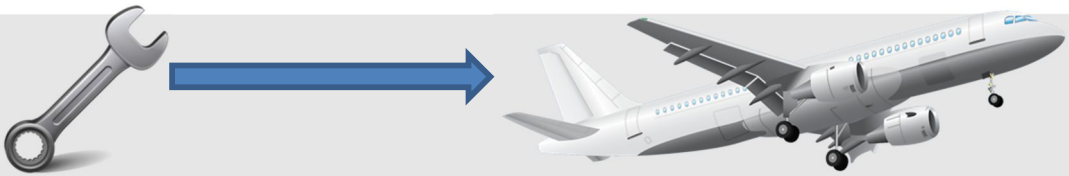


FBI-VICI Multi-core Analysis - UoY

Timing analysis of multi-core WCET interference

- **Knowledge Transfer Partnership** with Rolls-Royce (early adopter)
  - FBI being used to analyse interferences with the new generation of mixed-criticality scheduling
- **Industrial Avionics Working Group** (UK partners)
  - Investigating FBI to:
    - Provide evidence key properties of architectures hold in practice
    - Give support for both conventional and “living” safety cases
- **EPSRC research project** on Mixed-Criticality CPS
  - FBI as part of design and analysis of survivable comms
  - Aim is to understand how different factors affect the reliability, latency etc. of messages

RVS Qualification Kit Productization



How do you know you can trust the tool?

Before PROXIMA

After PROXIMA

New way of building RVS tool qualification kit that is: cheaper to make, easier for our customers (cheaper to use).

Is available on the market, has been sold and used several times.

Plan: sell more of them…

Exploitation Plan for Randomization Tech

Hardware	**Technology**: LEON3+ bitstream with extensions to model time-randomized caches and arbiters in the bus	**Exploitation**: CG can offer their customers processor designs and components based on PROXIMA technology CG has plans to include PROXIMA technology in some of its future processors
	Technology: libraries including RTL IP modules implementing the randomization technology	**Exploitation**: Can be provided-licensed to interested entities for evaluation of the randomization approach
Software	**Technology**: Dynamic SW randomization. Runtime that implements code, stack and global variables randomization	**Exploitation**: BSC and SYSGO are looking for joint projects to exploit DSR and further increase its TRL. Randomization can be applied to cover aspects related to security in cyber-physical systems .
	Technology: Static SW randomization. Stand-alone pre-compilation tool for achieving time randomization	**Exploitation** : BSC will offer this tool for test to industrial users as support for timing verification without altering current V&V processes.

Barcelona Supercomputing Center
Centro Nacional de Supercomputación

PROXIMA

Success Stories

Nov 22nd, 2016

This project and the research leading to these results has received funding from the European Community's Seventh Framework Programme [FP7 / 2007-2013] under grant agreement 611085

www.proxima-project.eu

What is a success story?

- Partnership
- Commercial activity
- Opportunity
- Product or service
- Further business
- Funding, knowledge transfer
- Route to exploitation

Multicore Timing Analysis Service

RAPITA Systems Ltd
A Danlaw Company

RVS tools
measures, optimizes & verifies the timing & test effectiveness of critical real-time systems

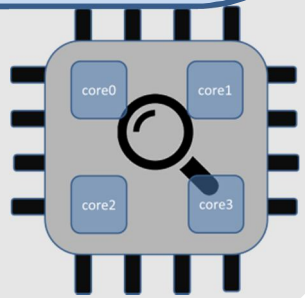
Barcelona Supercomputing Center
Centro Nacional de Supercomputación

Multicore knowledge:
+10 years of expertise in multicore timing analysis

micro-kernels:
specialized technology to find corner (timing) cases

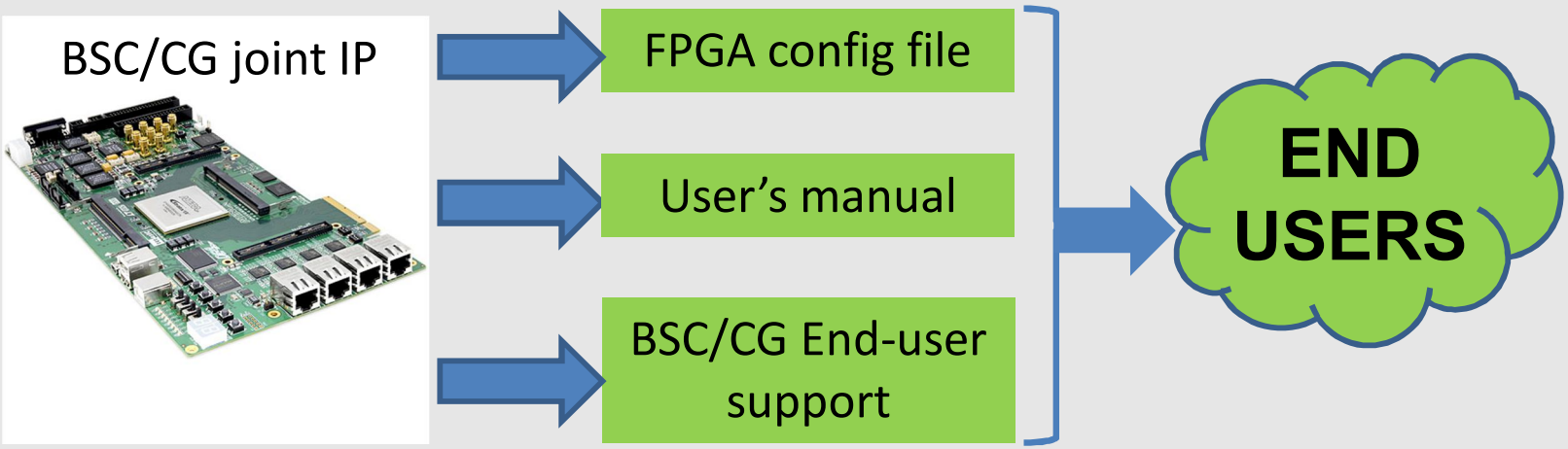
Technology: multicore timing analysis
Framework for the analysis of the processor timing of software running on multicores compliant with safety standard requirements

Exploitation
- New service offering
- Work for 3 aerospace & automotive customers in negotiation



BSC/CG partnership in the space domain

- Current commercial offering
  - [CG] PROXIMA's FPGA platform for evaluation to interested parties
    - FPGA configuration file for commercially available board
    - User's manual developed within PROXIMA
    - End-user support from CG or BSC based on user profile
  - Evaluation handled on a case-by-case basis
    - Use of the platform requires existing debug or evaluation license from CG
    - Commercial use likely to require support from both BSC and CG
  - [CG] processor designs based on the BSC/CG joint IP on HW-Rand, with support from BSC



BSC/CG partnership in the space domain

- New R&D
  - [CG/BSC] **joint research project with ESA** on shared cache including time-randomization
  - **From ESA** at ESA's ADCSS'16 workshop:
    - New approaches must be found: probabilistic timing analysis"
- PROXIMA technology available for existing space processor platform promoted through use in research projects
  - [CG/BSC] EFL-TR-CACHE
  - [UPD] RTEMS-SMP
- Further [CG/BSC] collaboration
  - Extended PMCs for multicore contention analysis in NGMP
  - **Privileged relationship**
    - BSC IP licensed to CG
    - CG providing BSC early access to its technology

PROXIMA

Industrial Partners' Exploitation Plans

Nov 22nd, 2016

This project and the research leading to these results has received funding from the European Community's Seventh Framework Programme [FP7 / 2007-2013] under grant agreement 611085

www.proxima-project.eu

Cobham Gaisler

- **Exploitation plan: PROXIMA output as additional feature set to support IP core library sales and for future devices.**
- **IP core library providing platform, including time-randomized processor**
  - LEON3-based bitstream for a time-randomized processor available now. Cobham Gaisler IP library – with patches for PROXIMA hardware randomization
  - Advertised at http://gaisler.com/leon3
- **The same PROXIMA technology has already been proposed in bids for standard product developments**
  - PROXIMA also enables collaboration between CG and BSC on bids.

SYSGO

EMBEDDING INNOVATIONS

Technologies

- **PikeOS LEOPARD BSP**:
  - On demand with PikeOS 3.4, candidate for a future PikeOS 4.X
- **Time Composable PikeOS communication ports**:
  - On demand with PikeOS 3.4, candidate for a future PikeOS 4.X
- **MBTA & MBPTA support** (PikeOS/RVS integration)**:**
  - On demand with PikeOS 3.4, candidate for a future PikeOS 4.X

Success Stories

- **PikeOS/RVS** integration:
  - opened new tools business in 2 major avionics suppliers

AIF

- Waiting for technology to be fully commercialized
  - Monitoring technology developments
- Ongoing research with INRIA
- Invited PROXIMA to present technology at a certification conference

Airbus Defence and Space Plan

AIRBUS DEFENCE & SPACE

On-going

- Internal promotion
- Lobbying on agencies to adopt PTA
  - ESA already involved in PROXIMA
  - CNES in progress

2017

- CNES will issue an ITT next year to continue research
  - Focus on ARM target
  - Use case: auto-coded AOCS
  - Technology: Software randomisation from PROXIMA

Rapita Systems Plan

RAPITA Systems Ltd
A BAE Systems Company

Technologies

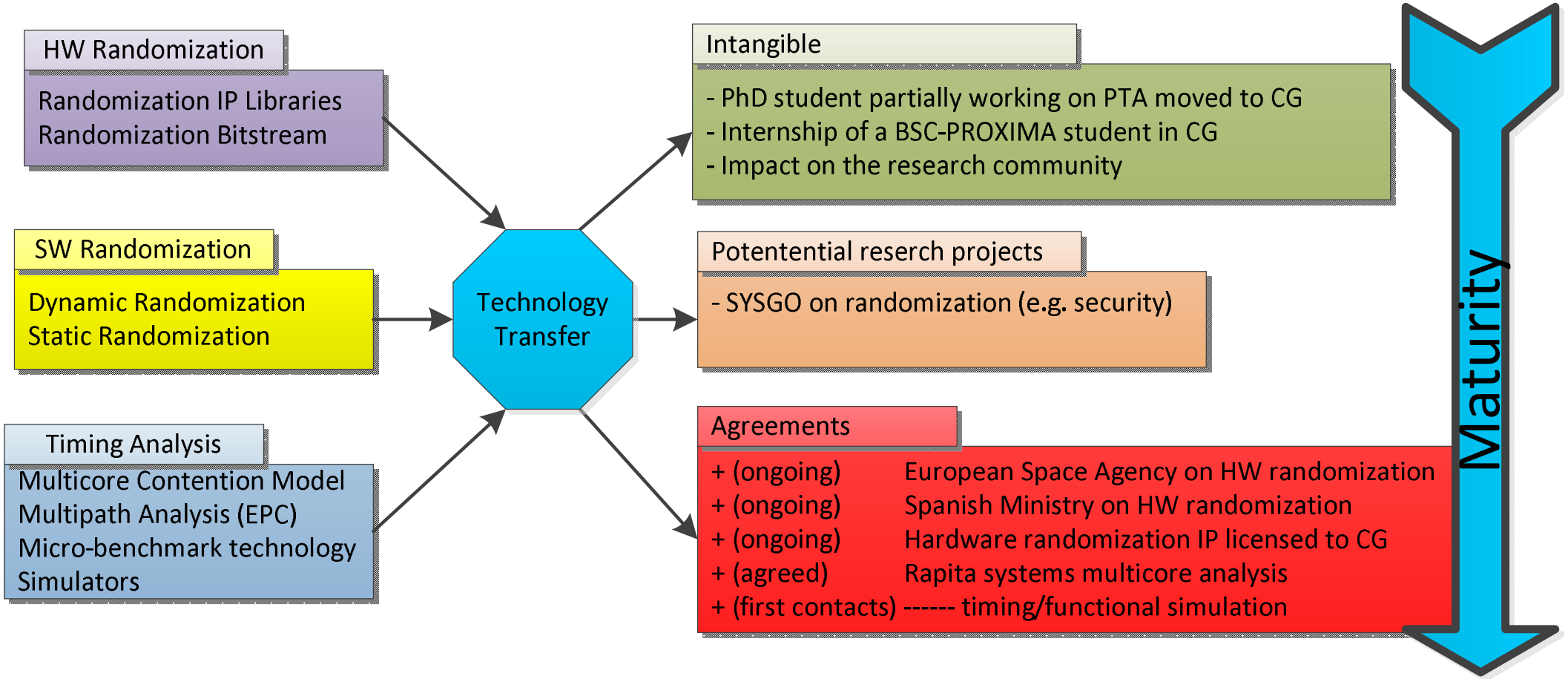
- **RVS QK product (aero market)**:
  - Sold already, certified on civil aeroplane. Plan: sell more…
- **RapiTime-PROXIMA**:
  - Some features to become as part of “time-bands” release in 2017. Early Access Programme.
- **Multi-core tracing:**
  - Now part of integration service (future business growth area), variant is now in use.

Success Stories

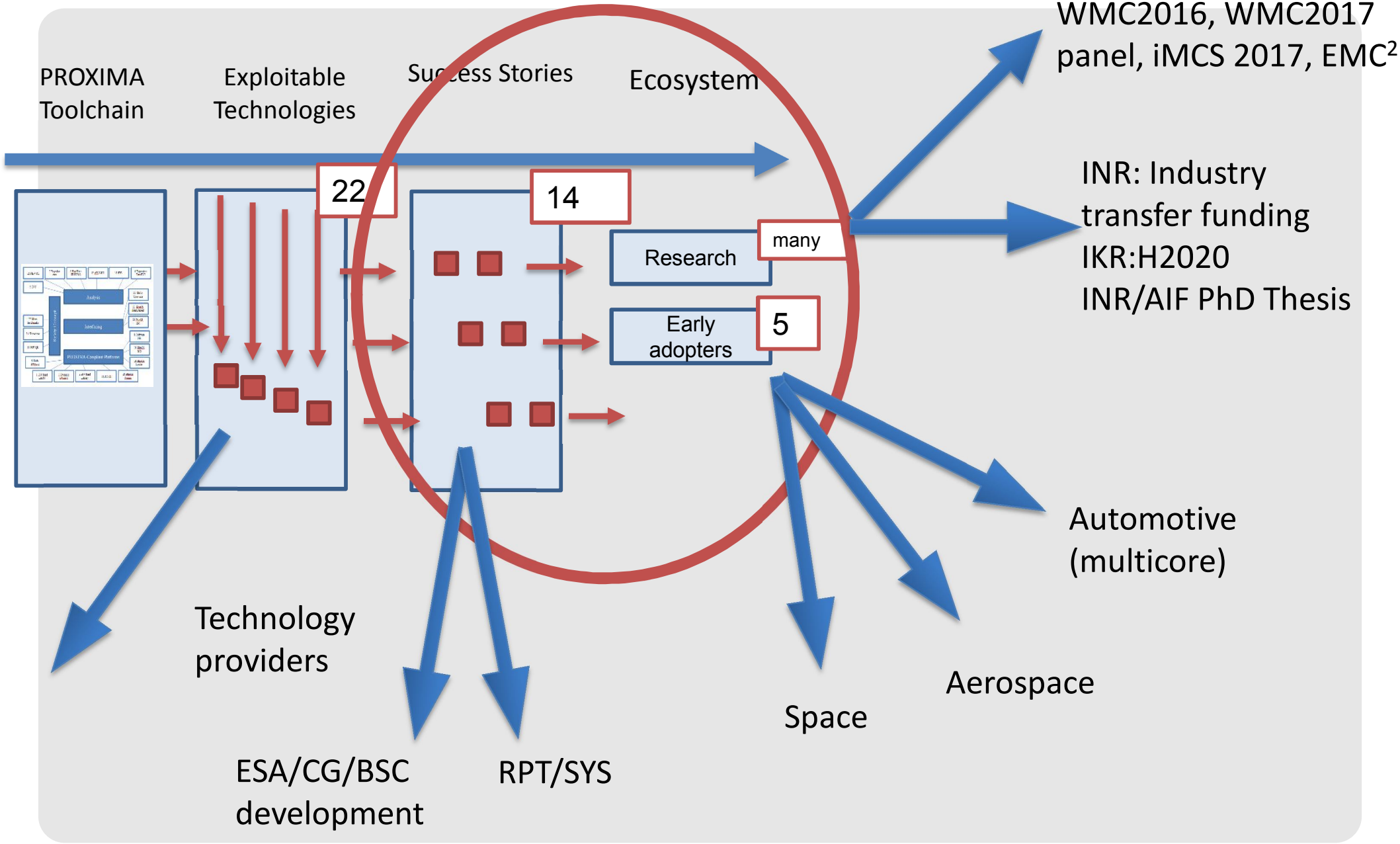
- **SYS/RPT PikeOS/RVS** integration:
  - Develop business in customers
- **BSC/RPT new multi-core services**
  - Opportunity with 3 customers

BSC: Transferring Technologies

- We have developed
  - HW/SW randomization technologies
  - multicore contention model
  - timing analysis techniques
  - Simulation infrastructures
- Different readiness for industrial transfer
- Exploitation approach identified for all them



PROXIMA


PROXIMA Toolchain
Exploitable Technologies
Success Stories
Ecosystem
22
14
Research
many
Early adopters
5
Dagstuhl, RTSS, WMC2016, WMC2017 panel, iMCS 2017, EMC²
INR: Industry transfer funding
IKR:H2020
INR/AIF PhD Thesis
Automotive (multicore)
Aerospace
Space
Technology providers
ESA/CG/BSC development
RPT/SYS

PROXIMA

MCC Workshop

Adriana Gogonel

PROXIMA dissemination WP leader representative
INRIA expert on EVT

BSC-UPC, Nov 22nd, 2016

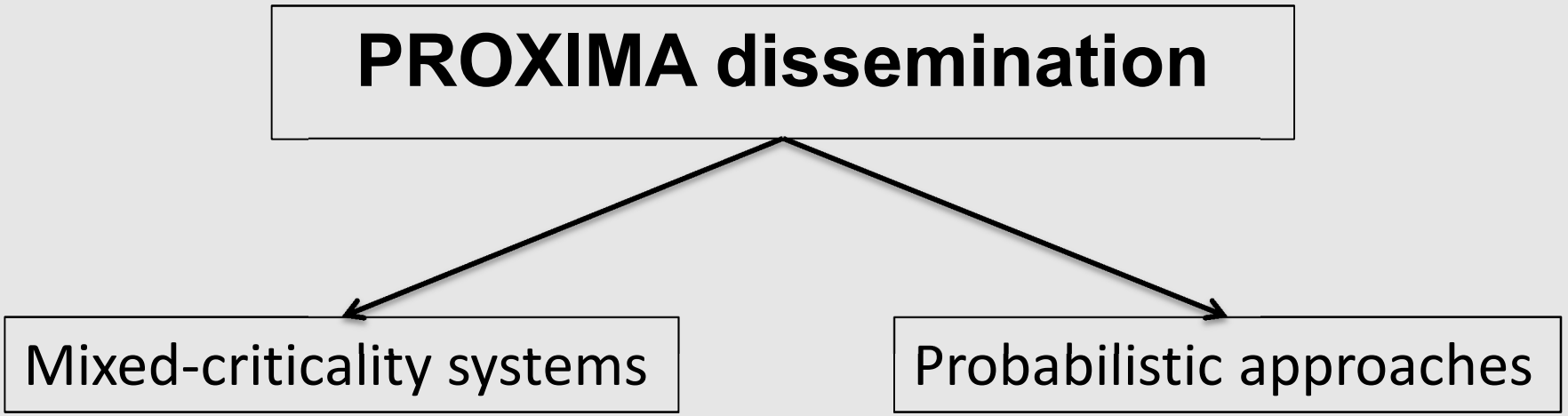
This project and the research leading to these results has received funding from the European Community's Seventh Framework Programme [FP7 / 2007-2013] under grant agreement 611085

www.proxima-project.eu

MIXED-CRITICALITY CLUSTER

Contrex DREAMS PROXIMA

SEVENTH FRAMEWORK PROGRAMME



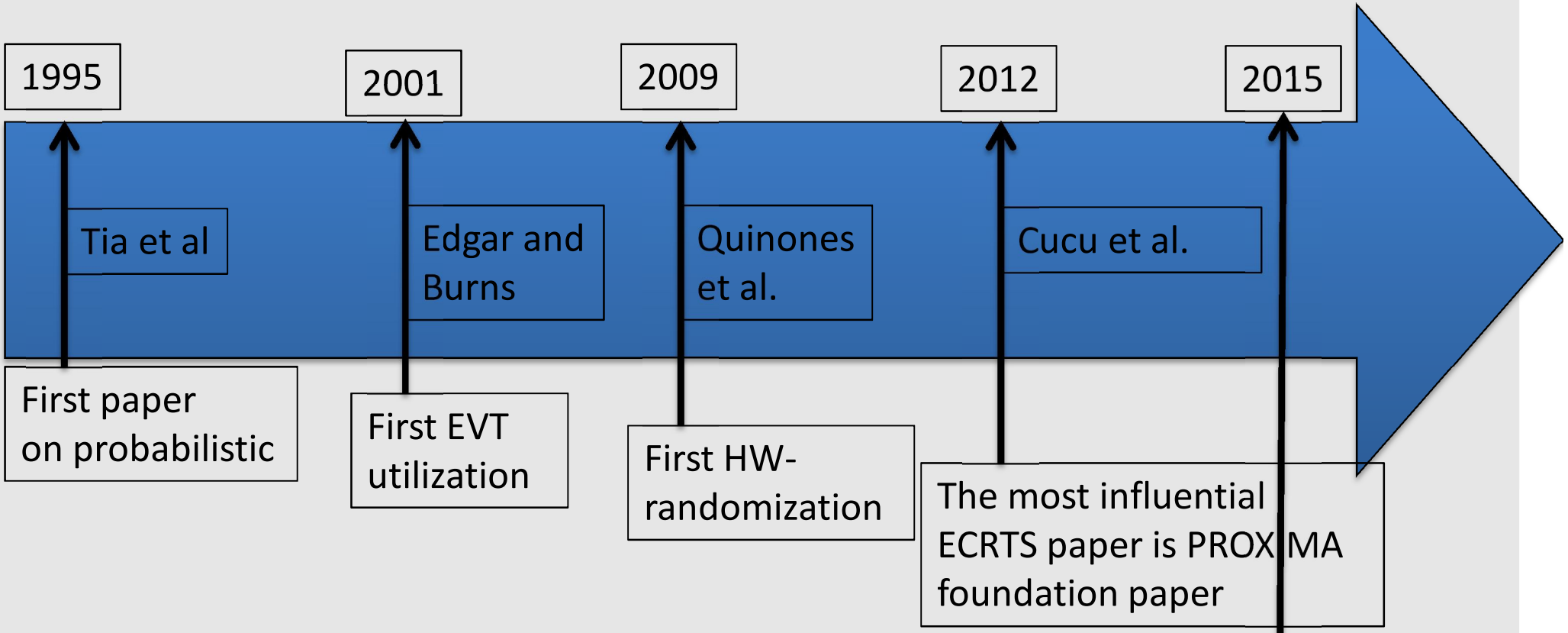
Building a mixed-criticality community

- ✓ **WMC**: 4 editions
  - ➢ RTSS workshop
    - Largest number of participants
    - Largest number of submitted papers
  - ➢ Proposed and co-organized by **PROXIMA dissemination leader**

- ✓ **Dagstuhl seminar on mixed-criticality** : 2 editions
  - ➢ The most prestigious event in Computer Science
  - ➢ Proposed and co-organized by **PROXIMA dissemination leader**

- ✓ **Challenges in Mixed Criticality**
  - Thematic session on MC at Hipeac CSW 2014
  - Proposed and co-organized **by PROXIMA leader**

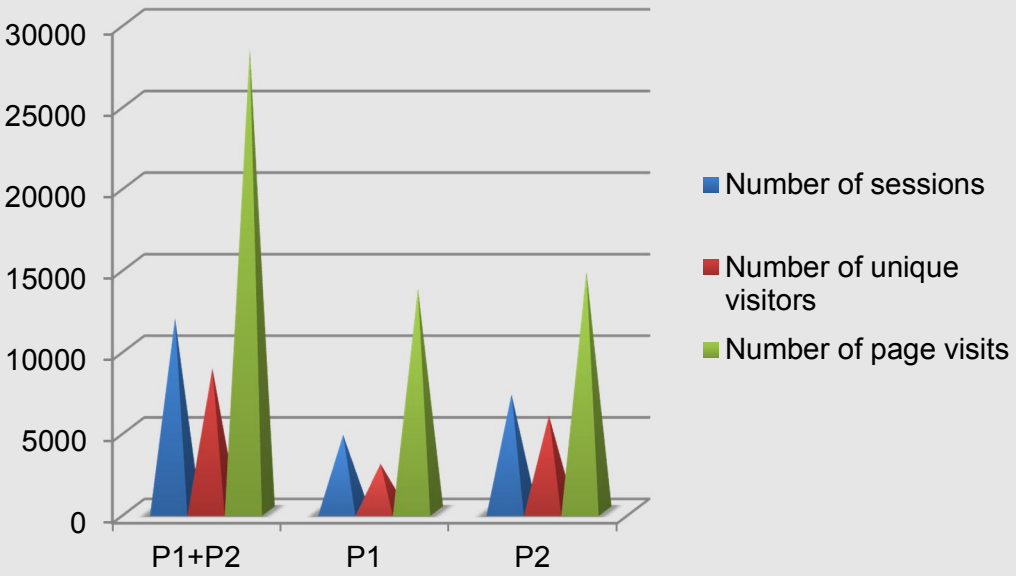
Consolidating the recognition of probabilistic



56 accepted papers

- 7 journal papers
- 38 conference papers
- 11 workshop papers

Important dissemination impact



The PROXIMA final industry workshops has attracted more than 20 international experts

Innovation Europe

GOOD TIMING: PROXIMA RESULTS TO HAVE WIDE-RANGING IMPACT

The EU FP7 IP PROXIMA project has recently concluded having worked for the last three years on the development of probabilistic software timing analysis and tools for multicore platforms. Its goal has been to reduce the cost of software timing verification for mixed-criticality and multicore systems.

PROXIMA focused on two main areas of work: timing analysis tools using probabilistic techniques to predict program timing behaviour; and methods to improve testability of real-time systems using injection of randomization into the timing behaviour of certain hardware/software. Covering both customized hardware designs and COTS technology, PROXIMA has been applied to several platforms including LEON3, AURIX and P4080.

PROXIMA

MCC Workshop

Adriana Gogonel

PROXIMA dissemination WP leader representative
INRIA expert on EVT

BSC-UPC, Nov 22nd, 2016

This project and the research leading to these results has received funding from the European Community's Seventh Framework Programme [FP7 / 2007-2013] under grant agreement 611085

www.proxima-project.eu